

On The Distribution Of The Signs Of Cyclotomic Units
Of A Cyclotomic Field.

Gordon Jones

A Thesis
in
The Department
of
Mathematics

Presented in Partial Fulfillment of the Requirements
for the degree of Master of Science at
Concordia University
Montréal, Québec, Canada

August 1983,

© Gordon Jones, 1983

ABSTRACT

On the Distribution of the Signs of Cyclotomic Units of a Cyclotomic Field

Gordon Jones

Let $K_m = Q(\zeta_m)$ be the cyclotomic field obtained by adjoining a primitive m^{th} root of unity ζ_m to the field of rational numbers Q . The unit group of K_m is denoted E_m . The maximal real subfield of K_m is denoted by K_m^+ where $K_m^+ = Q(\zeta_m + \zeta_m^{-1})$ and its group of units by E_m^+ . The cyclotomic units C_m form a subgroup of E_m of finite index. The cyclotomic units of K_m^+ are $C_m^+ = K_m^+ \cap C_m$. We denote by Z a subgroup of C_m^+ with generators $\epsilon_1, \dots, \epsilon_n$, $n = \phi(m)/2$. The ϵ_i are given in the text.

Let $G = G(K_m^+/Q)$ denote the Galois group of K_m^+ over Q . A mapping $\text{sgn}_\sigma: E_m^+ \rightarrow \mathbb{F}_2$ is defined for each $\sigma \in G$ and $\mu \in E_m^+$.

The matrix $M = (\text{sgn}_{\sigma_j}(\epsilon_i))$, $\sigma_j \in G$, $\epsilon_i \in Z$, is called the matrix of cyclotomic signatures. The rank of this matrix determines the sign distribution of the conjugates of the units of the subgroup Z of the cyclotomic units. The rank of M was computed for two different unit groups Z of the field K_m^+ where K_m^+ is a field in the tower of fields, $K_q^+ \subseteq K_{q \cdot 2^2}^+ \subseteq K_{q \cdot 2^3}^+ \subseteq \dots \subseteq K_{q \cdot 2^n}^+ \subseteq \dots$, q an odd integer. The results appear in the tables.

INDEX OF NOTATIONS

\mathbb{C}	field of complex numbers
C_m^+	the cyclotomic units of K_m^+
C_m'	Ramachandra's units p. 10 (Theorem 8)
C_m''	a subgroup of C_m^+ p. 10 (Theorem 7)
d_m	the order of the matrix M minus the rank of M
E_m	unit group of $K_m = \mathbb{Q}(\zeta_m)$
E_m^+	unit group of $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$
F	field K_m^+
\mathbb{F}_2	Galois field of two elements
$\mathbb{F}_2[G(F/Q)]$	group ring of $G(F/Q)$ over \mathbb{F}_2
$\phi(m)$	Euler phi function
$G(L/K)$	Galois group of L over K
K^*	non-zero elements of field K
M	matrix of cyclotomic signatures p. 20
q	an odd rational integer
\mathbb{Q}	field of rational numbers
$\text{sign}_\sigma(\alpha)$	σ -sign of α p. 20
$\text{sgn}_\sigma(\alpha)$	σ -signature of α p. 20
$\text{sgn}(\mu)$	see definition p. 24
ζ_m	primitive m^{th} root of unity
\mathbb{Z}	ring of rational integers
\mathbb{Z}	a subgroup of the cyclotomic units C_m^+
$ \cdot $	ordinary absolute value
$[\cdot]$	least positive residue mod x
(\div)	Legendre symbol

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	i
INDEX OF NOTATIONS	ii
TABLE OF CONTENTS	iii
ACKNOWLEDGEMENTS	iv
CHAPTER 1: Cyclotomic Fields	1
CHAPTER 2: Rings of Integers	3
CHAPTER 3: Units	4
CHAPTER 4: The Cyclotomic Units	8
CHAPTER 5: Matrix of Signatures	20
CHAPTER 6: The Signature Map	24
CHAPTER 7: Survey of Results	28
REFERENCES	31
APPENDIX-TABLES	32

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. H. Kisilevsky for his encouragement and advice in the preparation of this thesis.

Also, I wish to thank Richard Parker who helped with the Fortran program, and finally, I am grateful to Ilana Crawford for typing the thesis.

CHAPTER 1

CYCLOTOMIC FIELDS

CHAPTER 1

CYCLOTOMIC FIELDS

Let $\zeta_m = e^{2\pi i/m}$ be a primitive m^{th} root of unity, i.e. $\zeta_m^m = 1$ while $\zeta_m^a \neq 1$ for $1 \leq a < m$. Then $K_m = Q(\zeta_m)$ is the cyclotomic field of m^{th} roots of 1, where $m \geq 2$ is any integer such that $m \neq 2 \pmod{4}$, Q the field of rational numbers. The following theorem, which describes the Galois group $G(K_m/Q)$ of K_m over Q , is well known.

Theorem 1

K_m/Q is an abelian extension of degree $\phi(m)$; in fact, $G(K_m/Q)$ is isomorphic to the multiplicative group of integers $(\text{mod } m)$ which are relatively prime to m [that is, to $(Z/mZ)^*$, Z the ring of rational integers]. The conjugates of $\zeta = \zeta_m$ are precisely the primitive m^{th} roots of 1, and $f(\zeta, Q) = \prod_{\substack{(a,m)=1 \\ 1 \leq a < m}} (x - \zeta^a)$, is the minimal polynomial of ζ over Q .

Proof: See Weiss [14], p. 255.

The isomorphism referred to in the Theorem is given by $a \rightarrow \sigma_a$ where $(a, m) = 1$, $1 \leq a < m$ and $\sigma_a(\zeta_m) = \zeta_m^a$, also $\sigma_b = \sigma_a$ iff $b \equiv a \pmod{m}$. Now $G(Q(\zeta_m)/Q)$ contains an element σ_{-1} of order 2, namely the element such that $\sigma_{-1}(\zeta_m^a) = \zeta_m^{-a} = \overline{\zeta_m^a}$ where $\bar{\alpha}$ denotes the complex conjugate of $\alpha \in C$, where C is the field of complex numbers. Thus σ_{-1} is the automorphism of $G(Q(\zeta_m)/Q)$ defined by complex conjugation. Now, σ_{-1} has order 2, the fixed field of σ_{-1} which we denote by $Q(\zeta_m)^+$, is a real field, actually the maximal real subfield of $K = Q(\zeta_m)$, and $[Q(\zeta_m) : Q(\zeta_m)^+] = 2$, while $[Q(\zeta_m)^+ : Q] = \phi(m)/2$. We will show that $Q(\zeta_m)^+ = Q(\zeta_m + \zeta_m^{-1})$. Now, $Q(\zeta_m + \zeta_m^{-1})$ is a real field which is fixed under σ_{-1} , therefore

$Q(\zeta_m + \zeta_m^{-1}) \subseteq Q(\zeta_m)^+$. Since ζ_m is a root of the polynomial $x^2 - (\zeta_m + \zeta_m^{-1})x + 1$, we have $[Q(\zeta_m) : Q(\zeta_m + \zeta_m^{-1})] \leq 2$. While $Q(\zeta_m) \supseteq Q(\zeta_m)^+ \supseteq Q(\zeta_m + \zeta_m^{-1})$ implies that:

$$[Q(\zeta_m) : Q(\zeta_m + \zeta_m^{-1})] \geq [Q(\zeta_m) : Q(\zeta_m)^+] = 2.$$

Thus $[Q(\zeta_m) : Q(\zeta_m + \zeta_m^{-1})] = 2$ and so we have, $Q(\zeta_m)^+ = Q(\zeta_m + \zeta_m^{-1})$.

Corollary 1.1

The maximal real subfield $F = Q(\zeta_m + \zeta_m^{-1})$ of the m^{th} cyclotomic field is a Galois extension of Q which has a Galois group $G(F/Q)$ which is abelian of order $\phi(m)/2$. In fact $G(Q(\zeta_m + \zeta_m^{-1})/Q) \cong G(Q(\zeta_m)/Q) / \langle \sigma_{-1} \rangle$.

Automorphisms of $Q(\zeta_m)^+$ over Q are obtained by restricting the automorphisms of $Q(\zeta_m)$ over Q to $Q(\zeta_m)^+$. Under this restriction two elements of any coset of the subgroup $\langle \sigma_{-1} \rangle$ in $G(Q(\zeta_m)/Q)$ may be identified.

In the following we will assume that automorphisms of $Q(\zeta_m)^+$ over Q have been obtained in this way.

CHAPTER 2

RINGS OF INTEGERS

CHAPTER 2

RINGS OF INTEGERS

Let L be a field, K a subfield of L . Then $\alpha \in L$ is said to be algebraic over K if α satisfies a non zero polynomial with coefficients in K . i.e. there exists $f(x) \in K[x]$ such that $f(\alpha) = 0$; dividing by the leading coefficient, we may assume f is monic. In otherwords, there exist elements $b_1, \dots, b_n \in K$, $n > 0$, such that $\alpha^n + b_1\alpha^{n-1} + \dots + b_n = 0$.

A complex number x is an algebraic number if it is algebraic over the field Q of rational numbers. An algebraic number which is a root of a monic polynomial with coefficients in the ring Z of rational integers is called an algebraic integer.

Theorem 2

The numbers $1, \zeta_m, \dots, \zeta_m^{\phi(m)-1}$ form an integral basis, a Z basis, for the ring of algebraic integers A_K in $Q(\zeta_m)$. i.e. $A_K = Z[\zeta_m]$.

Proof: See Ribenboim [11], p. 269.

Corollary 2.1

The real numbers $\zeta_m + \zeta_m^{-1}, \dots, \zeta_m^{\phi(m)} + \zeta_m^{-\phi(m)}$, form an integral basis for the ring of algebraic integers in $F = Q(\zeta_m + \zeta_m^{-1})$. i.e.

$$A_F = Z[\zeta_m + \zeta_m^{-1}].$$

Proof: See Washington [13], p. 16.

CHAPTER 3

UNITS

CHAPTER 3

UNITS

Definition: If $a \in A_K$ and there exists $b \in A_K$ such that $a \cdot b = 1$, then a is called a unit of the ring of algebraic integers A_K .

We have the following fact concerning the units of the ring of algebraic integers.

Theorem 3

An algebraic integer is a unit if and only if its norm $N(x) = \pm 1$,

where $N(x) = \prod_{i=1}^n \sigma_i(x)$.

Proof: If x is a unit, then there exists an algebraic integer x' such that $x \cdot x' = 1$. Taking norms we obtain $N(x) \cdot N(x') = 1$ since $N(x)$ and $N(x')$ are integers, therefore $N(x) = \pm 1$.

Conversely, if $N(x) = \pm 1$, then letting x' be the product of all conjugates of x distinct from x , we have $x \cdot x' = \pm 1$; but $x' = \sigma_2(x) \cdots \sigma_n(x)$ is a product of algebraic integers and is thus an algebraic integer, so x divides 1 in the ring A_K of algebraic integers. Therefore x is a unit.

Denote the set of all units of the algebraic number field K by U , then $U \subseteq A_K$.

If ζ_m is a root of unity, then ζ_m satisfies the polynomial $x^m - 1$, $m \geq 1$, and so ζ_m is an algebraic integer. Since $\zeta_m^m = 1$ then $\zeta_m^{-m} = 1$ and thus ζ_m^{-1} is also a root of unity. Thus any root of unity in K is a unit of A_K .

Let U denote the group of units of A_K and let W denote the subgroup of U consisting of roots of unity. W is a non-trivial subgroup of U , since $1, -1 \in W$.

We recall that, if the algebraic number field K is of degree n over the rational numbers Q , then there are precisely n distinct isomorphisms of this field into the field C of all complex numbers.

If the image of the field K under the isomorphism $\sigma: K \rightarrow C$ is contained in the real numbers, then the isomorphism σ is called real, and, if this is not the case, it is called complex.

If θ is a primitive element of the arbitrary algebraic number field K , which is a root of the irreducible polynomial $f(x)$ over Q , and if $\theta_1, \dots, \theta_n$ are the roots of $f(x)$ in the field C , then the isomorphism

$$K = Q(\theta) \rightarrow Q(\theta_i) \subset C, \quad (\theta \rightarrow \theta_i)$$

will be real if the root θ_i is real, and complex otherwise.

Let $\sigma: K \rightarrow C$ be a complex isomorphism. The mapping $\bar{\sigma}: K \rightarrow C$, defined by

$$\bar{\sigma}(x) = \overline{\sigma(x)}, \quad x \in K$$

is also a complex isomorphism of K into C . This isomorphism is called conjugate to σ . Since $\bar{\sigma} \neq \sigma$ and $\bar{\bar{\sigma}} = \sigma$, the set of all complex isomorphisms of K into C is divided into pairs of conjugate isomorphisms.

If among the isomorphisms of K into C there are r_1 real ones and $2r_2$ complex ones, then $r_1 + 2r_2 = n = [K:Q]$.

The following theorem, due to Dirichlet, gives the structure of the units U of A_K .

Theorem 4

The group U of units of the ring A_K of algebraic integers of K has the following structure

$$U \cong W \times C_1 \times \dots \times C_r,$$

where W is the cyclic group of order w of roots of unity belonging to K , each C_i is an infinite multiplicative cyclic group, and $r = r_1 + r_2 - 1$.

Proof: See Ribenboim [11], p. 148.

The units u_1, \dots, u_k of A_K are said to be multiplicatively independent whenever a relation:

$$u_1^{m_1} \cdot u_2^{m_2} \cdots u_k^{m_k} = 1, \text{ with } m_i \in \mathbb{Z},$$

is only possible when $m_1 = \dots = m_k = 0$. Thus Dirichlet's unit theorem says that there exists a root of unity ζ and r units of infinite order u_1, \dots, u_r , such that every unit u may be written uniquely in the form $u = \zeta^{e_0} \cdot u_1^{e_1} \cdots u_r^{e_r}$ with $0 \leq e_0 < w$ and $e_1, \dots, e_r \in \mathbb{Z}$.

Any set of r independent units $\{u_1, \dots, u_r\}$ of K , where $r = r_1 + r_2 - 1$, for which the above statement holds is called a fundamental system of units of K .

In the case of $K = \mathbb{Q}(\zeta_m)$, where $[K:\mathbb{Q}] = \phi(m)$, $\sigma(\zeta_m) = \zeta_m^a$, $(a, m) = 1$, $1 \leq a < m$ we have $r_1 = 0$, $r_2 = \phi(m)/2$ and therefore $r = \phi(m)/2 - 1$. While for $F = \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, where $[F:\mathbb{Q}] = \phi(m)/2$, and $\sigma(\zeta_m + \zeta_m^{-1}) = \zeta_m^a + \zeta_m^{-a}$, $(a, m) = 1$, $1 \leq a < m/2$, we have $r_1 = \phi(m)/2$, $r_2 = 0$ and thus $r = \phi(m)/2 - 1$. Thus the unit groups of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m)^+$ both have the same rank, $r = \phi(m)/2 - 1$.

Serge Lang [7], p. 84 gives the following definition of cyclotomic units.

Let m be the conductor of the cyclotomic field $\mathbb{Q}(\zeta_m)$, so either $m > 1$ is odd or m is divisible by 4. Let ζ be a primitive m^{th} root of unity. For b prime to m we let $g_b = (\zeta^b - 1)/(\zeta - 1)$.

Then g_b is a cyclotomic unit. That g_b is a unit follows from the fact that $g_b = (\zeta^b - 1)/(\zeta - 1) = \zeta^{b-1} + \zeta^{b-2} + \dots + \zeta + 1$ is an algebraic integer and $g_b^{-1} = (\zeta - 1)/(\zeta^b - 1) = (\zeta^{bk} - 1)/(\zeta^b - 1)$ for some k , since $(\mathbb{Z}/m\mathbb{Z})^*$ is a multiplicative group. Thus

$$g_b^{-1} = (\zeta^{kb} - 1)/(\zeta^b - 1) = \zeta^{(k-1)b} + \zeta^{(k-2)b} + \dots + \zeta^b + 1,$$

which is also an algebraic integer, and $g_b \cdot g_b^{-1} = 1$.

Therefore g_b is a unit. Without loss of generality we may assume that b is odd, since ζ_m^b depends only on the residue class of b mod m .

Then $g_b^+ = \zeta_m^{-v} \cdot g_b$ for $v = (b-1)/2$ is a real unit since ζ_m^{-v} and g_b are units and because $\sigma_{-1}(g_b^+) = g_b^+$.

The unit group generated by -1 and the units g_b^+ is referred to by Washington as C_m'' while the cyclotomic units of Washington are denoted by C_m . We will use Washington's notation. Washington ([13] in Prop. 2.8) demonstrates that $1 - \zeta_m$ is a unit of $\mathbb{Z}[\zeta_m]$ if m has at least two distinct prime factors.

CHAPTER 4

THE CYCLOTOMIC UNITS

CHAPTER 4

THE CYCLOTOMIC UNITS

To determine the unit group of an arbitrary algebraic number field is quite difficult. However, in the case of cyclotomic fields, a group of units is known, namely the cyclotomic units, which is of finite index in the full unit group. Moreover, this index is closely related to the class number.

Let V_m be the multiplicative group generated by $\{\pm \zeta_m, 1 - \zeta_m^a \mid 1 < a \leq m-1\}$. Let E_m be the group of units of $Q(\zeta_m)$ and define $C_m = V_m \cap E_m$. C_m is called the group of cyclotomic units of $Q(\zeta_m)$. The cyclotomic units of $Q(\zeta_m)^+$ can be defined as $C_m^+ = E_m^+ \cap C_m$, where E_m^+ is the group of units of $Q(\zeta_m)^+$. We do not know of generators for the full group of cyclotomic units of $Q(\zeta_m)^+$. Sinnott [12] has calculated the index of the full group of cyclotomic units to be:
 $[E_m^+ : C_m^+] = 2^b \cdot h_m^+$, where h_m^+ is the class number of $Q(\zeta_m)^+$ and $b = 0$ if $g = 1$ while $b = 2^{g-2} + 1 - g$ if $g \geq 2$, g the number of distinct prime factors of m .

Now $b = 0$ for $g = 1, 2$ and 3 , therefore $[E_m^+ : C_m^+] = h_m^+$ for $g = 1, 2, 3$.

Theorem 5

Let $m = p^\alpha$, p a prime and $\alpha \geq 1$.

- The cyclotomic units of $Q(\zeta_m)^+$ are generated by -1 and the units $\epsilon_a = \zeta_m^{(1-a)/2} \cdot (1 - \zeta_m^a)/(1 - \zeta_m)$, $1 < a \leq m/2$, $(a, p) = 1$.
- The cyclotomic units of $Q(\zeta_m)$ are generated by ζ_m and the cyclotomic units of $Q(\zeta_m)^+$.

Proof: See Washington [13], p. 144.

This theorem does not extend to the case where m is not a prime power. If m is not a prime power, not every cyclotomic unit is a product of roots of unity and numbers of the form $(1-\zeta^b)/(1-\zeta)$, with $(b,m) = 1$. Each such product is a real unit times a root of unity, while the cyclotomic unit $1-\zeta_m$ is not of this form. (See Washington's proof of Corollary 4.13 [13], p. 40).

In the case where m is a prime power, we have.

Theorem 6

Let p be a prime and $\alpha \geq 1$. The cyclotomic units $C_{p^\alpha}^+$ of $Q(\zeta_{p^\alpha})^+$ are of finite index in the full unit group $E_{p^\alpha}^+$, and $h_{p^\alpha}^+ = [E_{p^\alpha}^+ : C_{p^\alpha}^+]$, where $h_{p^\alpha}^+$ is the class number of $Q(\zeta_{p^\alpha})^+$.

Proof: See Washington [13], p. 145.

When m is not a prime power, the units of the form $\zeta^{(1-a)/2} \cdot (1-\zeta^a)/(1-\zeta)$ are not always multiplicatively independent.

A Dirichlet character is a multiplicative homomorphism $\chi: (Z/nZ)^* \rightarrow C^*$. If $n|m$ then χ induces a homomorphism $(Z/mZ)^* \rightarrow C^*$ by composition with the natural map $(Z/mZ)^* \rightarrow (Z/nZ)^*$. Thus we could consider χ as being defined mod m or mod n , since both are essentially the same map. It is convenient, however, to choose n minimal and call it the conductor of χ , denoted by f_χ . We will regard χ as a map $Z \rightarrow C$ by letting $\chi(a) = 0$ if $(a, f_\chi) \neq 1$. When χ is defined modulo its conductor, it is said to be a primitive character. A character χ is said to be even if $\chi(-1) = 1$, odd if $\chi(-1) = -1$. For $f_\chi = n$ we have $\chi(a)^{\phi(n)} = 1$ since $a^{\phi(n)} \equiv 1 \pmod{n}$, which means $\chi(a)$ is a root of unity.

Theorem 7

Let C_m'' be the group generated by -1 and the units of the form $\zeta_m^{(1-a)/2} (1-\zeta_m^a)/(1-\zeta_m)$, $1 < a < m/2$, $(a, m) = 1$. Then

$$[E_m^+ : C_m''] = h_m^+ \prod_{\chi \neq 1} \prod_{p|m} (1 - \chi(p)),$$

where χ runs through the nontrivial even characters mod m , and the index is infinite if the right-hand side is 0.

Proof: See Washington [13], p. 150.

Later we will examine certain conditions for the units above to be independent.

A set of units discovered by Ramachandra [10] can be used to show that the cyclotomic units are of finite index in the full group of units. Ramachandra's units differ from the units $(1-\zeta^a)/(1-\zeta)$ in that they contain contributions from the units of proper subfields.

Theorem 8

Let $n \not\equiv 2 \pmod{4}$, and let $n = \prod_{i=1}^S p_i^{e_i}$ be its prime factorization.

Let I run through all subsets of $\{1, \dots, S\}$, except $\{1, \dots, S\}$, and

let $n_I = \prod_{i \in I} p_i^{e_i}$. For $1 < a < n/2$, $(a, n) = 1$, define

$$\xi_a = \zeta_n^{d_a} \prod_I (1 - \zeta_n^{a n_I}) / (1 - \zeta_n^{n_I}), \quad d_a = \frac{1}{2}(1-a) \sum_I n_I.$$

Then $\{\xi_a\}$ forms a set of multiplicatively independent units for $Q(\zeta_n)^+$.

If C_n' denotes the group generated by -1 and the ξ_a 's and E_n^+ denotes the group of units of $Q(\zeta_n)^+$, then

$$[E_n^+ : C_n'] = h_n^+ \prod_{\chi \neq 1} \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \neq 0,$$

where h_n^+ is the class number of $Q(\zeta_n)^+$ and χ runs through the nontrivial even characters of $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof: See Washington [13], p. 147.

We have seen that the cyclotomic units of $Q(\zeta_{p^m})^+$ are generated by -1 and the units $\epsilon_a = \zeta_{p^m}^{(1-a)/2} \cdot (\zeta_{p^m}^a - 1) / (\zeta_{p^m} - 1)$, $1 < a < p^m/2$, $(a, p) = 1$ (Theorem 5).

We have also seen (Theorem 6) that these cyclotomic units are of finite index in the full unit group $E_{p^m}^+$. The result on Ramachandra's units Theorem 8; shows that $\{\epsilon_a\}$ forms a set of multiplicatively independent units for $Q(\zeta_{p^m})^+$.

We wish to show that for $m = q \cdot 2^n$, q odd, $n \geq 3$, the units ϵ_a of Theorem 7 where $\epsilon_a = \zeta_m^{(1-a)/2} \cdot (\zeta_m^a - 1) / (\zeta_m - 1)$ are independent if and only if $q = p^\alpha$, p an odd prime, $\alpha \geq 1$ and 2 is a primitive root mod p^β , for all β such that, $1 \leq \beta \leq \alpha$. It is well known that if g is a primitive root of p and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root of p^α for all α .

We will also show for $m = p^\alpha \cdot 2^2$, when the units ϵ_a are dependent if $p \equiv 1, 3$ or $5 \pmod{8}$ while for $p \equiv 7 \pmod{8}$, they are sometimes dependent, sometimes independent.

It was proved in Theorem 7 that C_m'' , the group generated by -1 and the units

$$\epsilon_a = \zeta_m^{(1-a)/2} \cdot \frac{\zeta_m^a - 1}{\zeta_m - 1}, \quad 1 < a < \frac{m}{2}, \quad (a, m) = 1$$

was of index $[E_m^+ : C_m''] = h_m^+ \prod_{\chi \neq 1} \prod_{p|m} (1 - \chi(p))$, in the full unit group E_m^+ , where χ runs through the nontrivial even characters mod m , and the index is infinite if the right hand side is 0. Hence $[E_m^+ : C_m'']$ is infinite if, and only if $\chi(p) = 1$, for some χ . Therefore we need only

consider those χ for which $(p, f_\chi) = 1$, since if $(p, f_\chi) \neq 1$ then $\chi(p) = 0$.

For $f_\chi = 1$ or 2, since $\phi(f_\chi) = 1$, the only character is the trivial character $\chi = 1$. While for $f_\chi = 4$, the only even character is the trivial one.

Consider $f_\chi = 2^b$, $b \geq 3$, we have from Apostol [1] p. 221, that the Dirichlet character

$$\chi_{a,c}(n) = \begin{cases} (-1)^{(n-1) \cdot a/2} \cdot e^{2\pi i b(n)c/2^{b-2}}, & n \text{ odd} \\ 0, & \text{if } n \text{ is even} \end{cases}$$

where $a = 1, 2$ and $c = 1, 2, \dots, \phi(2^b)/2$, is primitive mod 2^b if, and only if, c is odd, where $b(n)$ is the uniquely determined integer, such that $n \equiv (-1)^{(n-1)/2} 5^{b(n)} \pmod{2^b}$, with $1 \leq b(n) \leq \phi(2^b)/2$. A simple calculation shows that $\chi_{a,c}$ is even if, and only if, $a = 2$.

Thus for $f_\chi = 2^b$ the nontrivial even characters are

$$\chi_{2,c}(n) = \begin{cases} e^{2\pi i b(n)c/2^{b-2}}, & n \text{ odd} \\ 0, & \text{if } n \text{ is even} \end{cases}$$

For $f_\chi = p^a$, $1 \leq a \leq \beta$. Let g be a primitive root mod p which is also a primitive root mod p^k for all $k \geq 1$. Such a g exists by Theorem 10.6

(Apostol [1]). If $(n, p) = 1$ let $b(n) = \text{ind}_g n \pmod{p^a}$, so that $b(n)$

is the unique integer satisfying the conditions $n \equiv g^{b(n)} \pmod{p^a}$,

$0 \leq b(n) < \phi(p^a)$. For h such that $0 \leq h < \phi(p^a) - 1$, define χ_h by the

formula

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\phi(p^a)} & \text{if } p \nmid n \\ 0 & \text{if } p \mid n \end{cases}$$

then χ_h is a Dirichlet character mod p^a , with χ_0 being the trivial character. Apostol proves [1], p. 221, that χ_h is primitive if and only if $p \nmid h$. It can be shown that χ_h is even if and only if h is even.

For all a such that $(a, m) = 1$, a is called a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If it has no solution, then a is called a quadratic nonresidue modulo m .

If p denotes an odd prime and $(a, p) = 1$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue, -1 if a is a quadratic nonresidue modulo p .

Lemma 9.1 $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Proof: Niven and Zuckerman [9], p. 65.

It follows easily that $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3$ or $5 \pmod{8}$ while $\left(\frac{2}{p}\right) = 1$ when $p \equiv 1$ or $7 \pmod{8}$.

Lemma 9.2

If 2 is a primitive root mod p then $p \equiv 3$ or $5 \pmod{8}$.

Proof: $2^{p-1} \equiv 1 \pmod{p}$

$$(2^{(p-1)/2} + 1)(2^{(p-1)/2} - 1) \equiv 0 \pmod{p}$$

and since the factors differ by 2, therefore exactly one factor is divisible by p . Since 2 is a primitive root mod p , therefore

$$2^{(p-1)/2} \not\equiv 1 \pmod{p} \text{ so that } 2^{(p-1)/2} \equiv -1 \pmod{p} \text{ but}$$

$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ implies $\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv -1 \pmod{p}$ which means that $p \equiv 3$ or $5 \pmod{8}$.

Lemma 9.3

A number prime to p^a is a quadratic residue of p^a if and only if it is a quadratic residue of p .

Proof: See LeVeque [8], p. 63.

Theorem 9

If $m = p^\alpha \cdot 2^\beta$, $\alpha \geq 1$, $\beta \geq 3$ then the unit group C_m'' with generators -1 and $\epsilon_a = \zeta_m^{(1-a)/2} \cdot (\zeta_m^a - 1)/(\zeta_m - 1)$, $(a, m) = 1$, $1 < a < m/2$ is of finite index in the full group of units E_m^+ if and only if 2 is a primitive root mod p^a for all a , such that $1 < a \leq \alpha$.

Proof: We have seen that $[E_m^+ : C_m''] = h_m^+ \prod_{\chi \neq 1} \prod_{p|m} (1 - \chi(p))$ and that the index is finite if and only if $\chi(p) \neq 1$. We consider the nontrivial even characters with $f_\chi = 2^b$, $3 \leq b \leq \beta$.

$\chi_{2,c}(n) = e^{2\pi i b(n)c/2^{b-2}}$, c odd and $b(n)$ determined by $n \equiv (-1)^{(n-1)/2} \cdot 5^{b(n)} \pmod{2^b}$. The index is infinite if and only if $\chi(p) = 1$ for some χ and p . But $\chi_{2,c}(p) = 1$ if and only if $2^{b-2} | b(n)$ while $1 \leq b(n) \leq 2^{b-2}$ implies that $\chi_{2,c}(p) = 1$ if and only if $b(p) = 2^{b-2}$. For $p = 8k + 1$ or $8k + 7$ the formula $n \equiv (-1)^{(n-1)/2} \cdot 5^{b(n)} \pmod{2^b}$ gives the result $1 \equiv 5^{b(p)} \pmod{8}$. But $\text{ord}_{2^b} 5 = 2^{b-2}$ (see LeVeque [8] p. 54), therefore $b(p) = 2^{b-2}$ which implies that $\chi_{2,c}(p) = 1$ and the index $[E_m^+ : C_m'']$ is infinite. If $p = 8k + 3$ or $8k + 5$ it happens that $b(p) \neq 2^{b-2}$ and therefore $\chi_{2,c}(p) \neq 1$. We have seen, Lemma 10.2, that if 2 is a primitive root mod p then $p \equiv 3$ or $5 \pmod{8}$. The converse is not true as 2 is neither a primitive root mod 43 nor mod 109.

Consider the case $p \equiv 3$ or $5 \pmod{8}$, 2 a primitive root mod p^a . We have seen that $\chi_{2,c}(p) \neq 1$. If $f_\chi = p^a$, $1 \leq a \leq \alpha$, then

$$\chi_h(n) = e^{2\pi i h b(n)/\phi(p^a)}, \quad n \equiv g^{b(n)} \pmod{p^a},$$

since we can put $g = 2$ therefore $b(2) = 1$.

Therefore $\chi_h(2) = e^{2\pi i h / \phi(p^a)}$, $2 \leq h \leq \phi(p^a) - 2$ with h even.
 $\chi_h(2) = 1$ if and only if $\phi(p^a) \mid h$ which is impossible. Thus $\chi_h(2) \neq 1$.

Of course $\chi_h(p) = 0$ and $\chi_{2,C}(2) = 0$. Thus if 2 is a primitive root mod p^a for all a , such that $1 \leq a \leq \alpha$, then $[E_m^+ : C_m'']$ is finite.

Consider the case $p \equiv 3$ or $5 \pmod{8}$, 2 not a primitive root mod p^a for some a , with $1 \leq a \leq \alpha$. By Lemma 9.1, $p \equiv 3$ or $5 \pmod{8}$ implies $\left(\frac{2}{p}\right) = -1$, thus in $2 \equiv g^{b(2)} \pmod{p^a}$, $b(2)$ is odd (see Lemma 9.3). Since 2 is not a primitive root mod p^a , we have $2^k \equiv 1 \pmod{p^a}$, $k = \text{ord}_{p^a} 2$, $0 < k < \phi(p^a)$ and $k \mid \phi(p^a)$. Thus $k \cdot x = \phi(p^a)$ and $x = \phi(p^a)/k > 1$. Also from $2^k \equiv 1 \pmod{p^a}$ and $2 \equiv g^{b(2)} \pmod{p^a}$ we deduce that $g^{k \cdot b(2)} \equiv 2^k \equiv 1 \pmod{p^a}$, and so $\phi(p^a) \mid k \cdot b(2)$ or $\phi(p^a) \cdot y = k \cdot b(2)$ thus $k \cdot x \cdot y = k \cdot b(2)$ and $x \cdot y = b(2)$.

So $x \mid b(2)$ and $x \mid \phi(p^a)$, with $x > 1$ and since $b(2)$ is odd, then so also is x . For $p \equiv 3$ or $5 \pmod{8}$, 2 not a primitive root of p^a we have $p^a \geq 43$ and so $\phi(p^a) \geq 42$, since $x \geq 3$ we have $2x/(x-1) \leq 3$, thus $\phi(p^a) > 2x/(x-1)$ and therefore $\phi(p^a)/x < \phi(p^a) - 2$.

For $\chi_h(2) = e^{2\pi i h b(2) / \phi(p^a)}$, with $h = \phi(p^a)/x$ we have h even, $2 \leq h \leq \phi(p^a) - 2$ and $\chi_h(2) = 1$. Therefore if $p \equiv 3$ or $5 \pmod{8}$, and 2 is not a primitive root mod p^a , then the index $[E_m^+ : C_m'']$ is infinite.

What happens to the index $[E_m^+ : C_m'']$ if $m = q \cdot 2^\beta$, $\beta \geq 3$, q odd but having more than one prime divisor?

Theorem 10

For $m = q \cdot 2^\beta$, $\beta \geq 3$, q odd with at least two distinct prime divisors, the index $[E_m^+ : C_m'']$ is infinite.

Proof: If for any prime divisor p of q , it happens that 2 is not a

primitive root mod p , then as seen in the proof of Theorem 9, there exists χ such that $\chi(p) = 1$.

Suppose that, for all p dividing q , 2 is a primitive root mod p . Then $p \equiv 3$ or $5 \pmod{8}$ and we consider $f_\chi = p$. If χ_{h_1} and χ_{h_2} are both odd characters with $(f_{\chi_{h_1}}, f_{\chi_{h_2}}) = 1$, then $\chi = \chi_{h_1} \cdot \chi_{h_2}$ is an even character with $f_\chi = f_{\chi_{h_1}} \cdot f_{\chi_{h_2}}$.

If $\chi_h(n) = e^{2\pi i h b(n)/(p-1)}$, $n \equiv g^{b(n)} \pmod{p}$ it is easy to show that χ_h is odd if and only if h is odd. Since 2 is a primitive root for each $p|q$, we have $b(2) = 1$. If $p \equiv 3 \pmod{8}$, then in $\chi_h(2) = e^{2\pi i h/(p-1)}$, take $h = (p-1)/2$. Thus we have h odd, $1 \leq h \leq p-2$ and $\chi_h(2) = -1$. So if q has at least two distinct divisors each of which is congruent to 3 mod 8, we are done. Suppose this is not the case. Perhaps q has no divisors congruent to 3 mod 8. Then q has at least two distinct prime factors congruent to 5 mod 8. Therefore in $\chi_{h_i}(2) = e^{2\pi i h_i/(p_i-1)}$, let $h_i = (p_i-1)/2$, so that h_i is even, $1 \leq h_i \leq p_i-2$ and $\chi_{h_i}(2) = -1$. So again $\chi = \chi_{h_1} \cdot \chi_{h_2}$ is even and $\chi(2) = 1$. What if q has prime factors p_1 and p_2 , with p_1 congruent to 3 mod 8 and p_2 congruent to 5 mod 8. Whether $p \equiv 3$ or $5 \pmod{8}$ we have for $f_\chi = 8$, that $b(p) = 1$ and $\chi_{2,C}(p) = -1$. Now since 2 is a primitive root of both p_1 and p_2 we have $p_1 \equiv 2^{b(p_1)} \pmod{p_2}$.

In $\chi_h(n) = e^{2\pi i h b(n)/(p-1)}$, for $f_\chi = p_2$, where $p_2 \equiv 5 \pmod{8}$ let $h = (p_2-1)/2$. Then h is even and $1 \leq h \leq p_2-2$, while

$$\chi_h(p_1) = e^{2\pi i h b(p_1)/(p_2-1)} = e^{\pi i b(p_1)} = \pm 1.$$

If $\chi_h(p_1) = 1$, we are done. If not, define $\chi = \chi_h \cdot \chi_{2,C}$ and so

$$\chi(p_1) = \chi_h(p_1) \cdot \chi_{2,C}(p_1) = (-1) \cdot (-1) = 1.$$

We now examine the index $[E_m^+ : C_m^+]$ for $m = q \cdot 2^2$, q odd.

Corollary 9.1

If $m = p^\alpha \cdot 2^2$, $\alpha \geq 1$ with $p \equiv 3$ or $5 \pmod{8}$ then $[E_m^+ : C_m'']$ is finite if and only if 2 is a primitive root of p^a , $1 \leq a \leq \alpha$.

Proof: See the proof of Theorem 9.

Theorem 11

For $m = p^\alpha \cdot 2^2$, the index $[E_m^+ : C_m'']$ is infinite if $p \equiv 1 \pmod{8}$.

Proof: For $p \equiv 1 \pmod{8}$, $f_\chi = p$, then $\chi_h(2) = e^{2\pi i h b(2)/(p-1)}$ and $h = (p-1)/2$ is even. Since $(\frac{2}{p}) = 1$, therefore $b(2)$ is even. Thus $\chi_h(2) = 1$ and the index is infinite.

For $m = p^\alpha \cdot 2^2$, $p \equiv 7 \pmod{8}$ the situation is not so clear. When $m = 7 \cdot 2^2$, $[E_m^+ : C_m'']$ is finite, while for $m = 31 \cdot 2^2$ the index $[E_m^+ : C_m'']$ is infinite.

Corollary 11.1

If $m = q \cdot 2^2$, q odd with $p|q$ such that

a) $p \equiv 3$ or $5 \pmod{8}$ and 2 is not a primitive root of p .

or b) $p \equiv 1 \pmod{8}$

then the index $[E_m^+ : C_m'']$ is infinite.

Proof: a) See the proof of Theorem 9.

b) See proof of Theorem 11.

Theorem 12

If $m = q \cdot 2^2$, q odd and p_1 and p_2 are divisors of q such that.

$p_1, p_2 \equiv 3$ or $7 \pmod{8}$, then the index $[E_m^+ : C_m'']$ is infinite.

Proof: For $p \equiv 3 \pmod{8}$, let $f_\chi = p$.

Then $\chi_h(2) = e^{2\pi i h b(2)/(p-1)}$ and if $h = (p-1)/2$ we have h odd, and since $(\frac{2}{p}) = -1$, $b(2)$ is odd. Therefore $\chi_h(2) = -1$, χ odd.

For $p \equiv 7 \pmod{8}$, $f_{\chi} = p$ let $h = (p-1)/2$ so that h is odd and $\chi_h(2) = e^{2\pi i h b(2)/(p-1)}$ and since $(\frac{2}{p}) = 1$, $b(2)$ is even, thus $\chi_h(2) = 1$ with χ odd.

So if p_1 and p_2 are both congruent to 3 or both congruent to 7 mod 8, then $\chi = \chi_{h_1} \cdot \chi_{h_2}$, $h_i = (p_i-1)/2$ and χ is even with $\chi(2) = \chi_{h_1}(2) \cdot \chi_{h_2}(2) = 1$.

Assume $p_1 \equiv 3 \pmod{8}$, $p_2 \equiv 7 \pmod{8}$, then by the law of quadratic reciprocity, $(p_1/p_2)(p_2/p_1) = -1$. Without loss of generality assume $(p_1/p_2) = -1$, then in $\chi_h(p_1) = e^{2\pi i h b(p_1)/(p_2-1)}$ with $h = (p_2-1)/2$ an odd number and $\chi_h(p_1) = e^{\pi i b(p_1)} = -1$ since $b(p_1)$ is odd. For $f_{\chi} = 4$, $\chi'(p_1) = -1$. Both χ_h and χ' are odd, therefore $\chi = \chi_h \cdot \chi'$ is even and $\chi(2) = 1$.

Theorem 13

If $m = q \cdot 2^2$, q odd and p_1 and p_2 are distinct prime divisors of q . Then the index $[E_m^+ : C_m'']$ is infinite if either;

- i) $p_1, p_2 \equiv 5 \pmod{8}$, 2 a primitive root of p_1 and p_2 .
- ii) $p_1 \equiv 5 \pmod{8}$ with 2 a primitive root of p_1 , $p_2 \equiv 3$ or $7 \pmod{8}$ and $(p_2/p_1) = 1$.

Proof:

- i) For $f_{\chi} = p_i$, $i = 1, 2$.

$\chi_h^i(2) = -1$ for $h_i = (p_i-1)/2$, χ_h^i even, define $\chi = \chi_h^1 \cdot \chi_h^2$, then χ is even and $\chi(2) = 1$.

- ii) For $f_{\chi} = p_1$, $\chi_h(p_2) = (-1)^{b(p_2)}$ for $h = (p-1)/2$. So χ is even and if $(p_2/p_1) = 1$ then $\chi_h(p_2) = 1$.

If in Theorem 13ii, $(p_2/p_1) = -1$ then $[E_m^+ : C_m'']$ is not necessarily infinite. For example if $m = 3 \cdot 5 \cdot 2^2$ or $m = 7 \cdot 5 \cdot 2^2$ then $[E_m^+ : C_m'']$ is

finite, while $[E_m^f : C_m^f]$ is infinite if $m = 11 \cdot 5 \cdot 2^2$ or $m = 31 \cdot 5 \cdot 2^2$.

Consider $m = p^\alpha \cdot 2^\beta$, p a fixed odd prime, $\alpha \geq 1$ also fixed, $\beta \geq 2$.

Since $(n, f_\chi) \neq 1$ implies $\chi(n) = 0$, therefore if we are to have $\chi(q) = 1$ for q a prime such that $q|m$ then either, $q = p$ and $f_\chi = 2^b$ or $q = 2$ and $f_\chi = p^a$.

Theorem 14

There are only finitely many even characters mod $m = p^\alpha \cdot 2^\beta$, such that $\chi(q) = 1$, where $q = p$ or 2 .

Proof: If χ is an even character mod p^α then $f_\chi = p^a$, $1 \leq a \leq \alpha$. But there are only $\phi(p^a)$ characters with conductor $f_\chi = p^a$, and therefore only finitely many even characters mod p^α , such that $\chi(2) = 1$.

If χ is an even character mod 2^β then $f_\chi = 2^b$, $2 \leq b \leq \beta$, and $\chi_{2,C}(n) = e^{2\pi i b(n)C/2^{b-2}}$ with $n \equiv (-1)^{(n-1)/2} \cdot 5^{b(n)} \pmod{2^b}$. Now $\chi_{2,C}(p) = 1$ if and only if $b(p) = 2^{b-2}$ which implies $p \equiv (-1)^{(p-1)/2} \pmod{2^b}$ or equivalently $p \pm 1 \equiv 0 \pmod{2^b}$. But there exists b_0 such that $2^{b_0} > p + 1$, and therefore $p \pm 1 \not\equiv 0 \pmod{2^b}$ so that $\chi_{2,C}(p) \neq 1$ for any χ with $f_\chi = 2^b$, $b \geq b_0$. Thus all the even characters mod 2^β , $\beta \geq 2$ for which $\chi_{2,C}(p) = 1$ have conductor f_χ where $f_\chi = 2^b$, $2 \leq b \leq b_0$. Thus there are only finitely many $\chi_{2,C}$ that are trivial at p .

Table 3 gives, for some values of m , the number of χ for which $\chi(q) = 1$.

CHAPTER 5

MATRIX OF SIGNATURES

CHAPTER 5

MATRIX OF SIGNATURES

Let $\sigma \in G(F/Q)$, where $F = Q(\zeta_m + \zeta_m^{-1})$ and let $\alpha \in F^*$. Let $|x|$ represent the ordinary absolute value of the real number x . Then we will call $\text{sign}_\sigma(\alpha) = \sigma(\alpha)/|\sigma(\alpha)|$ the σ -sign of α . If $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$, $n = \phi(m)/2$ is a fixed but arbitrary ordering of $G(F/Q)$ then we call the n -tuple $(\text{sign}_{\sigma_1}(\alpha), \text{sign}_{\sigma_2}(\alpha), \dots, \text{sign}_{\sigma_n}(\alpha))$ the $G(F/Q)$ -sign of α . And if the map $\rho: \{1, -1\} \rightarrow F_2$ is defined by $\rho(-1) = 1$, $\rho(1) = 0$, then we call $\text{sgn}_\sigma(\alpha) = \rho(\text{sign}_\sigma(\alpha))$ the σ -signature of α . We call the n -tuple $(\text{sgn}_{\sigma_1}(\alpha), \dots, \text{sgn}_{\sigma_n}(\alpha))$ the $G(F/Q)$ -signature of α . The sign and signature functions exhibit the sign behavior of the conjugates of α .

The square matrix $M = (m_{ij})$ where $m_{ij} = \text{sgn}_{\sigma_j}(\epsilon_i)$, $\sigma_j \in G(F/Q)$, ϵ_i one of the generators of the unit group Z (where Z is either C' or C'' etc.) with, $1 \leq i \leq m/2$, $(i, m) = 1$ exhibits the sign structure of the units Z .

Since we will be interested only in the rank of M , therefore we may choose any convenient ordering of the Galois group $G(F/Q)$. The elements of $G(F/Q)$ can be chosen as coset representatives of the cosets of the subgroup $\langle \sigma_{-1} \rangle$, generated by complex conjugation in $G(Q(\zeta_m)/Q)$. The elements σ_a and σ_{m-a} with $(a, m) = 1$, $1 \leq a < m/2$ belong to the same coset of $G(F/Q)$ since $\sigma_a(\zeta_m)$ is the conjugate of $\sigma_{m-a}(\zeta_m)$. Thus we can represent $G(F/Q)$ as $\{\sigma_a \mid (a, m) = 1, 1 \leq a < m/2\}$ where $\sigma_a(\zeta_m) = \zeta_m^a$.

Consider $Z = C_m''$. For the purposes of calculation we will choose $\zeta_m = e^{2\pi i/m} = \cos 2\pi/m + i \sin 2\pi/m$. Now $\epsilon_1 = -1$ and

$$\epsilon_a = \zeta_m^{(1-a)/2} \cdot (\zeta_m^a - 1)/(\zeta_m - 1), \quad (a, m) = 1, 1 \leq a < m/2 \text{ and } \zeta_m = \zeta_{2m}^2$$

where we take $\zeta_{2m} = e^{2\pi i/2m} = \cos 2\pi/2m + i \sin 2\pi/2m$ then

$$\epsilon_a = (\zeta_{2m}^2)^{(1-a)/2} \cdot \frac{\zeta_{2m}^{2a} - 1}{\zeta_{2m}^2 - 1} = \frac{\zeta_{2m}^{-a}}{\zeta_{2m}^{-1}} \cdot \frac{\zeta_{2m}^{2a} - 1}{\zeta_{2m}^2 - 1}$$

$$\text{thus } \epsilon_a = \frac{\zeta_{2m}^a - \zeta_{2m}^{-a}}{\zeta_{2m} - \zeta_{2m}^{-1}} = \frac{2i \sin \frac{2\pi}{2m} \cdot a}{2i \sin \frac{2\pi}{2m}}$$

$$\text{therefore } \epsilon_a = \frac{\sin \frac{2\pi}{2m} \cdot a}{\sin \frac{2\pi}{2m}}, \text{ hence}$$

$$\sigma_j(\epsilon_i) = \frac{\zeta_{2m}^{ij} - \zeta_{2m}^{-ij}}{\zeta_{2m}^j - \zeta_{2m}^{-j}} = \frac{\sin 2\pi(\frac{ij}{2m})}{\sin 2\pi(\frac{j}{2m})}$$

We define a function

$$[\cdot] : \mathbb{Z} \rightarrow \{k \mid (k, x) = 1, 0 \leq k < x\}$$

by $[\ell] = q$ for $\ell \in \mathbb{Z}$, $q \in \{k \mid (k, x) = 1, 0 \leq k < x\}$

if and only if $\ell \equiv q \pmod{x}$.

That is, $[\ell]$ is the least positive residue of $\ell \pmod{x}$.

For the case of m even, let a be an arbitrary integer such that $(a, 2m) = 1$. Then the sign of $\sin 2\pi(a/2m)$ is determined by the least positive residue of $a \pmod{2m}$. That is

$$\frac{\sin 2\pi(\frac{a}{2m})}{|\sin 2\pi(\frac{a}{2m})|} = \begin{cases} +1 & \text{if } 0 < [a] < m \\ -1 & \text{if } m < [a] < 2m. \end{cases}$$

$$\text{Therefore } \text{sign}_{\sigma_j}(\epsilon_i) = \begin{cases} +1 & \text{if } 0 < [ij] < m \\ -1 & \text{if } m < [ij] < 2m \end{cases}$$

$$\text{and } \text{sgn}_{\sigma_j}(\epsilon_i) = \begin{cases} 0 & \text{if } 0 < [ij] < m \\ 1 & \text{if } m < [ij] < 2m \end{cases}$$

Also we have $\text{sgn}_{\sigma_j}(\epsilon_1) = 1$ for all σ_j since $\epsilon_1 = -1$.

Thus the matrix M is given by $M = (m_{ij})$ where $m_{ij} = \text{sgn}_{\sigma_j}(\epsilon_i)$ and $m_{1j} = 1$ for $j \in \{x | (x, m) = 1, 1 \leq x < m/2\}$

$$\text{and } m_{ij} = \begin{cases} 0 & \text{if } 0 < [ij] < m \\ 1 & \text{if } m < [ij] < 2m \end{cases}$$

with j as before and

$$i \in \{x | (x, m) = 1, 1 < x < m/2\}.$$

For m odd, we have as generators of $\mathbb{Z} = \mathbb{C}_m^u$ $\epsilon_1 = -1$,

$\epsilon_a = \zeta_m^{(1-a)/2} \cdot (\zeta_m^a - 1) / (\zeta_m - 1)$, $(a, m) = 1$, $1 < a < m/2$ where ζ_m is a primitive m^{th} root of unity. But for m odd ζ_m^2 is also a primitive m^{th} root of unity. Replace ζ_m by ζ_m^2 . We get

$$\epsilon_a = \zeta_m^{1-a} \frac{\zeta_m^{2a} - 1}{\zeta_m^2 - 1} = \frac{\zeta_m^a - \zeta_m^{-a}}{\zeta_m - \zeta_m^{-1}}$$

We are thus replacing ϵ_a by $\sigma_2(\epsilon_a)$, where $\sigma_2 \in G(Q(\zeta_m)^+/Q)$. The matrix of cyclotomic signatures is given by $M = (\rho(\sigma_b(\epsilon_a)))$, thus becomes

$M = (\rho(\sigma_b(\sigma_2(\epsilon_a))))$ or $M = (\rho(\sigma_{2b}(\epsilon_a)))$ where $\sigma_{2b} \in G$. So we have only rearranged the elements of the Galois group of $Q(\zeta_m)^+/Q$, that is the columns of the matrix will be rearranged. So $M = (\rho(\sigma_j(\epsilon_i)))$, where

$$\sigma_j(\epsilon_i) = \frac{\zeta_m^{ij} - \zeta_m^{-ij}}{\zeta_m^j - \zeta_m^{-j}} = \frac{\sin 2\pi(\frac{ij}{m})}{\sin 2\pi(\frac{j}{m})}$$

therefore $M = (m_{ij})$; with $m_{1j} = 1$ and

$$m_{ij} = \begin{cases} 0 & \text{if } 0 < [ij] < \frac{m}{2} \\ 1 & \text{if } \frac{m}{2} < [ij] < m \end{cases}$$

$$i \in \{x | (x, m) = 1, 1 < x < \frac{m}{2}\}$$

$$j \in \{x | (x, m) = 1, 1 \leq x < \frac{m}{2}\}$$

A FORTRAN program was used and executed on a VAX to determine the matrix and its rank for several values of m . See the tables for results.

CHAPTER 6

THE SIGNATURE MAP

CHAPTER 6

THE SIGNATURE MAP

Let $E = E_m^+$ represent the group of units of $F = Q(\zeta_m)^+$ and denote by $Z = C_m''$ the subgroup of the cyclotomic units, which is described in Theorem 7.

An element $\mu \in E$ is totally positive, denoted $\mu \gg 0$, if and only if, for all automorphisms $\sigma \in G(F/Q)$, $\sigma(\mu) > 0$. An element μ in E is a square if and only if there exists a unit v in E such that $\mu = v^2$.

Let $E^+ = \{\mu \mid \mu \in E, \mu \text{ is totally positive}\}$

$E^2 = \{\mu \mid \mu \in E, \mu \text{ is a square}\}.$

Lemma 15.1

The sets E^+ and E^2 are multiplicative subgroups of E and $E^2 \subseteq E^+$.

Proof: See D. Davis [3], p. 10.

Consider the group ring $\mathbb{F}_2[G(F/Q)]$ of the Galois group of F over Q over the Galois field of two elements. Let sgn be the mapping from the units E to $\mathbb{F}_2[G(F/Q)]$ defined by

$$\text{sgn}(\mu) = \sum_{\sigma \in G(F/Q)} \text{sgn}_{\sigma}(\mu) \cdot \sigma, \mu \in E$$

$$\text{where } \text{sgn}_{\sigma}(\mu) = \begin{cases} 0 & \text{if } \sigma(\mu) > 0 \\ 1 & \text{if } \sigma(\mu) < 0 \end{cases}$$

Lemma 15.2

The mapping $\text{sgn}: E \rightarrow \mathbb{F}_2[G(F/Q)]$ is a homomorphism of groups and $\ker \text{sgn} = E^+$.

Proof: D. Davis [10], p. 10.

Theorem 15

The dimension of $\text{sgn}(\mathbb{Z})$ as a vector space over \mathbb{F}_2 equals the rank of the matrix M of cyclotomic signatures.

Proof: D. Davis [10], p. 11.

Corollary 15.1

The number of even invariants of the group \mathbb{Z}/\mathbb{Z}^+ equals the rank of the matrix of cyclotomic signatures.

Proof: D. Davis [3], p. 11.

Theorem 16

The homomorphism $\text{sgn}: E \rightarrow \mathbb{F}_2[G(F/Q)]$ is onto if and only if $E^2 = E^+$.

Proof: D. Davis [3], p. 11.

Corollary 16.1

If the matrix M of cyclotomic signatures is non-singular over \mathbb{F}_2 , then $E^2 = E^+$.

Proof: D. Davis [3], p. 11.

We will denote by d_m the difference between the order of the matrix M and its rank.

Lemma 17.1

If $\mu \in \mathbb{Z}$ such that $\mu \gg 0$ and $\mu = \epsilon_1^{a_1} \dots \epsilon_r^{a_r}$, not all the a_i even, the ϵ_i generators of \mathbb{Z} , then $d_m \geq 1$.

Proof: If $\mu \notin \mathbb{Z}^2$ then the result follows from Corollary 16.1. If $\mu \in \mathbb{Z}^2$ then since $\mu \gg 0$, therefore $\text{sgn}(\mu) = \sum_{\sigma \in G} \text{sgn}_{\sigma}(\mu) \cdot \sigma = 0$, if and only if

$$(\text{sgn}_{\sigma_1}(\mu), \dots, \text{sgn}_{\sigma_r}(\mu)) = 0, \text{ iff}$$

$$a_1(\text{sgn}_{\sigma_1}(\epsilon_1), \dots, \text{sgn}_{\sigma_r}(\epsilon_1)) + \dots + a_r(\text{sgn}_{\sigma_1}(\epsilon_r), \dots, \text{sgn}_{\sigma_r}(\epsilon_r)) = 0.$$

Since the a_i are not all even, therefore there is a linear combination of

rows of the matrix M equal to zero. Thus $d_m \geq 1$.

Let E_K represent the group of units of the algebraic number field K of degree n over Q . For r elements $\epsilon_1, \dots, \epsilon_r$ of E_K , $r = r_1 + r_2 - 1$, we define the regulator $R(\epsilon_1, \dots, \epsilon_r)$ as follows. Write the isomorphisms of K into C as $\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \dots, \sigma_{r+1}, \bar{\sigma}_{r_1+1}, \dots, \bar{\sigma}_{r+1}$, where σ_j , $1 \leq j \leq r_1$, is real, and $\sigma_j, \bar{\sigma}_j$, $r_1 + 1 \leq j \leq r + 1$, is a pair of complex isomorphisms. Let $\delta_j = 1$ if σ_j is real and $\delta_j = 2$ if σ_j is complex. The regulator of $(\epsilon_1, \dots, \epsilon_r)$ is defined as,

$$R(\epsilon_1, \dots, \epsilon_r) = \left| \det(\delta_j \log |\epsilon_i|) \right|_{1 \leq i, j \leq r}.$$

In order for $\epsilon_1, \dots, \epsilon_r$ to be multiplicatively independent, it is necessary and sufficient that $R(\epsilon_1, \dots, \epsilon_r) \neq 0$. (see Cohn [2], p. 112)

Now, in the proof of Corollary 8.8 Washington ([3], p. 150), gives the following formula for the regulator of the generators of C_m'' .

$$R(\epsilon_1, \dots, \epsilon_r) = h_m^+ R_m^+ \prod_{\chi \neq 1} \prod_{p|m} (1 - \chi(p)), \quad (*)$$

where χ runs through the nontrivial even characters mod m , h_m^+ is the class number and R_m^+ is the regulator of $K_m^+ = Q(\zeta_m)^+$, where $R_m^+ = R(\mu_1, \dots, \mu_r)$, with the μ_i forming a basis for the group of units of $Q(\zeta_m)^+$ modulo $\{\pm 1\}$. Since h_m^+ and R_m^+ are not zero, therefore, $R(\epsilon_1, \dots, \epsilon_r) \neq 0$ if and only if the right hand side of (*) is not zero. That is; $R(\epsilon_1, \dots, \epsilon_r) \neq 0$ if and only if $[E_m^+ : C_m'']$ is finite. We thus have,

Lemma 17.2

The generators $\epsilon_a = \zeta_m^{(1-a)/2} (\zeta_m^a - 1) / (\zeta_m - 1)$ of C_m'' , $(a, m) = 1$, $1 < a < m/2$, are independent if and only if $[E_m^+ : C_m'']$ is finite.

Theorem 17

If $[E_m^+ : C_m'']$ is infinite then $d_m \geq 1$.

where d_m = order of M - rank of M .

Proof: If $[E_m^+ : C_m'']$ is infinite then the ϵ_a are multiplicatively dependent. Thus $\prod_a \epsilon_a^{x_a} = 1$, not all the x_a zero. Assume 2^k , $k \in \mathbb{Z}$ is the largest power of 2 dividing all the x_a , then

$$(\prod_a \epsilon_a^{x'_a})^{2^k} = 1, \quad x'_a = x_a / 2^k.$$

Since the ϵ_a are real, $\prod_a \epsilon_a^{x'_a} = \pm 1$. For $\epsilon_1 = -1$, let $\mu = \epsilon_1^{x'_1} \prod_{a \neq 1} \epsilon_a^{x'_a}$, with x'_1 chosen so that $\mu = 1$.

Thus, $\mu \in \mathbb{Z}$, $\mu \gg 0$ and $\mu = \prod_{\substack{1 \leq a \leq m/2 \\ (a,m)=1}} \epsilon_a^{x'_a}$, not all the x'_a even,

therefore by Lemma 17.1 we have $d_m \geq 1$.

CHAPTER 7

SURVEY OF RESULTS

CHAPTER 7

SURVEY OF RESULTS

We present here certain results due to Garbanati ([4],[5]) and Gras [6], which explain some features of the tables obtained for the Matrix M of cyclotomic signatures. $Z = C_m''$.

We have already seen that when C_m'' is not of finite index in E_m^+ then the matrix M of cyclotomic signatures is singular, i.e. $d_m > 1$. But even when $[E_m^+ : C_m'']$ is finite, $m = p^\alpha \cdot 2^\beta$, $\beta \geq 2$, we still have $d_m > 1$. Theorem 18 will deal with this situation. First we show two lemmas.

In "Unit Signatures and Class Numbers", Garbanati states ([4], p. 378) the following lemma, concerning a real abelian extension K of the rationals Q .

Lemma 18.1

If each prime p of Q which ramifies in K does not split then,

$|Z^+/Z^2| = 2^{n - \dim(\text{sgn } Z)}$, where n is the degree of the extension of K over Q and $\dim(\text{sgn } Z)$ is equal to the rank of the matrix M of signatures of C_m'' .

Proof: see Garbanati [4], p. 378.

We wish to determine for which $K_m^+ = Q(\zeta_m)^+$, $m = p^\alpha \cdot 2^\beta$, with $[E_m^+ : C_m'']$ finite, the lemma holds. $[E_m^+ : C_m'']$ finite with $\beta \geq 3$ implies $p \equiv 3$ or $5 \pmod{8}$ and that 2 is a primitive root of p .

The only primes that ramify in $K_m = Q(\zeta_m)$ are p and 2. But 2 does not split in K_m and thus 2 does not split in K_m^+ . If $p \equiv 3$ or $5 \pmod{8}$ then p splits into two factors in $K_m = Q(\zeta_m)$. Now $i = \zeta_4 \in K_m$ and $\sqrt{2} = \zeta_8 + \zeta_8^{-1} \in K_m = Q(\zeta_m)$ so that $Q(\sqrt{2})$, $Q(i)$ and $Q(\sqrt{-2})$ are quadratic

subfields of K_m . Also $Q(\sqrt{2}) \subseteq Q(\zeta_m + \zeta_m^{-1})$.

In $Q(\sqrt{d})$, p is decomposed if and only if $(d/p) = 1$. Thus for $p \equiv 1$ or $7 \pmod{8}$, p splits in $Q(\sqrt{2})$ since $(2/p) = 1$.

Therefore $p \equiv 1$ or $7 \pmod{8}$ splits in $Q(\zeta_m)^+$.

For $p \equiv 3 \pmod{8}$, $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$,

therefore $p \equiv 3 \pmod{8}$ splits in $Q(\sqrt{-2})$.

While for $p \equiv 5 \pmod{8}$, $\left(\frac{-1}{p}\right) = -1$, hence p splits in $Q(i)$.

So for $p \equiv 3$ or $5 \pmod{8}$ we have

$$pA_K = P_1 \cdot P_2, \text{ with } P_1 \neq P_2 \text{ and } N(P_1) = N(P_2) = p.$$

The two factors P_1 and P_2 of p are complex conjugates, thus $P_1, P_2 \notin Q(\zeta_m)^+$. Therefore $p \equiv 3$ or $5 \pmod{8}$ does not split in $K_m^+ = Q(\zeta_m)^+$. So for $p \equiv 3$ or $5 \pmod{8}$ 2 a primitive root of p , Lemma 18.1 holds.

Thus $|Z^+/Z^2| = 2^{n-\dim(\text{sgn} Z)}$ while $|E^+/E^2| = 2^{n-\dim(\text{sgn} E)}$ (see [4], p. 378). Since $E \supset Z$ then $\dim(\text{sgn} E) \geq \dim(\text{sgn} Z)$ and so it follows that $|Z^+/Z^2| \geq |E^+/E^2|$.

Lemma 18.2

Let K^+ be a real finite abelian extension of Q . If there exists an imaginary abelian extension K of Q such that $[K:K^+] = 2$ and K is an unramified extension of K^+ then $(E^+ : E^2) > 1$.

Proof: see Garbanati [5], p. 169.

Theorem 18

For $K_m^+ = Q(\zeta_m)^+$, $m = p^\alpha \cdot 2^\beta$, $\alpha \geq 1$, $\beta \geq 2$ with $p \equiv 3$ or $5 \pmod{8}$ and 2 a primitive root of p , then $d_m \geq 1$.

Proof: Since m is not a prime power, therefore K_m/K_m^+ is unramified ([13], p. 16) and so by lemma 18.2 $(E^+ : E^2) > 1$. By lemma 18.1 we have $|Z^+/Z^2| > |E^+/E^2| > 1$. Thus there exists $\mu \in \mathbb{Z}$ with $\mu > 0$, $\mu \notin \mathbb{Z}^2$ and lemma 17.1 implies that $d_m > 1$.

Lemma 19.1

If each prime p of Q which ramifies in K_m^+ does not split and if $|Z^+/Z^2| = 1$ then h is odd.

Proof: see Garbanati [4], p. 379.

Theorem 19

If $K_{p^\alpha}^+ = Q(\zeta_{p^\alpha})^+$, p an odd prime, then the only prime that ramifies is p and it does not split. If h_p^+ is even then lemma 19.1 implies that $|Z^+/Z^2| > 1$ and so by lemma 17.1 we have $d_m > 1$.

Gras has established a criterion for the parity of the class number of abelian extensions K/Q of odd degree. The criterion involves the signature of the cyclotomic units.

Let $\mu \in E$, μ is 2-primary if the extension $K(\sqrt{\mu})/K$ is non-ramified for prime ideals not dividing 2.

Let $Z_0 = \{\eta \in \mathbb{Z}, \eta \text{ is 2-primary}\}$.

Theorem 20

h is even if and only if

$$(Z^+/Z^2) \cap (Z_0/Z^2) \neq (1)$$

Proof: see Gras [6], p. 41.

Theorem 20 implies that when $|Z^+/Z^2| = 1$ then h is odd, while h even implies $|Z^+/Z^2| > 1$.

REFERENCES

REFERENCES

1. Apostol, Tom, "Introduction to Analytic Number Theory", Springer-Verlag, New York, 1976.
2. Cohn, Harvey, "A Classical Invitation to Algebraic Numbers and Class Fields", Springer Verlag, New York, 1978.
3. Davis, Daniel, "On the Distribution of the Signs of the Conjugates of the Cyclotomic Units in the Maximal Real Subfield of the q th Cyclotomic Field, q a Prime", Thesis, California Institute of Technology, 1969.
4. Garbanati, Dennis, "Unit Signatures, and Even Class Numbers, and Relative Class Numbers", J. reine angew. Math. 274/275 (1975), 376-384.
5. Garbanati, Dennis, "Units with Norm-1 and Signatures of Units", J. reine angew. Math., 283/284 (1976), 164-175.
6. Gras, George, "Parité du nombre de classes et unités cyclotomiques", Astérisque, 24-25 (1975), 37-45.
7. Lang, Serge, "Cyclotomic Fields", Springer Verlag, New York 1978.
8. LeVeque, W.J., "Topics in Number Theory, Vol. I", Addison-Wesley Publishing Company, Reading, Mass., 1965.
9. Niven, I. and Zuckermann, H.S., "An Introduction to the Theory of Numbers", John Wiley and Sons Inc., New York, 1972.
10. Ramachandra, K., "On the Units of Cyclotomics Fields", Acta Arith., 12 (1966), 165-173.
11. Ribenboim, Paulo, "Algebraic Numbers", Wiley-Interscience, John Wiley and Sons Inc., New York, 1972.
12. Sinott, W., "On the Stickelberger Ideal and the Circular Units of a Cyclotomic Field", Ann. of Math. (2), 108 (1978), 107-134.
13. Washington, Lawrence C., "Introduction to Cyclotomic Fields", Springer Verlag, New York, 1982.
14. Weiss, Edwin, "Algebraic Number Theory", McGraw Hill, Inc., New York, 1963.

APPENDIX-TABLES

TABLE I

RANK OF MATRIX OF SIGNATURES OF C_m''

For each odd integer q , $3 \leq q \leq 125$, the rank of the matrix of signatures of units of the unit group C_m'' ($m = q \cdot 2^n$ $n = 0, 2, 3, 4, \dots$) was calculated on a VAX computer. The program was written in Fortran IV by Richard Parker and later modified to handle odd values of m . The results for prime values were checked by comparison with the results from Davis' Thesis ([3], p. 70).

For each value of q the results for the matrices associated with C_m'' , $m = q \cdot 2^n$ are arranged as follows.

For each value of n , the first column p_n gives the order of the matrix M , while the second column r_n gives the rank of M and the third column d_n gives the difference of the two, i.e. $d_n = p_n - r_n$.

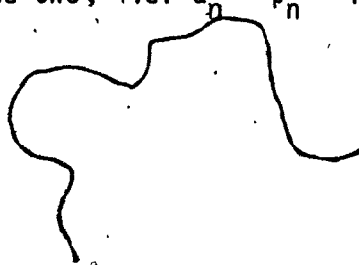


TABLE 1: C''_m

$q = 3$			$q = 5$			$q = 7$			$q = 3^2$			$q = 11$			$q = 13$			$q = 3.5$			$q = 17$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	1	1	0	2	2	0	3	3	0	3	3	0	5	5	0	6	6	0	4	3	1	8	8	0
2	2	1	1	4	3	1	6	5	1	6	5	1	10	9	1	12	11	1	8	5	3	16	14	2
3	4	3	1	8	7	1	12	10	2	12	11	1	20	19	1	24	23	1	16	11	5	32	29	3
4	8	7	1	16	15	1	24	21	3	24	23	1	40	39	1	48	47	1	32	23	9	64	59	5
5	16	15	1	32	31	1	48	45	3	48	47	1	80	79	1	96	95	1	64	55	9	128	119	9
6	32	31	1	64	63	1	96	93	3	96	95	1	160	159	1	192	191	1	128	119	9	256	239	17
7	64	63	1	128	127	1	192	189	3	192	191	1	320	319	1				256	247	9			
8	128	127	1	256	255	1																		
9	256	255	1																					

$q = 19$			$q = 3.7$			$q = 23$			$q = 5^2$			$q = 3^3$			$q = 29$			$q = 31$			$q = 3.11$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	9	9	0	6	5	1	11	11	0	10	10	0	9	9	0	14	11	3	15	15	0	10	9	1
2	18	17	1	12	9	3	22	21	1	20	19	1	18	17	1	28	24	4	30	27	3	20	17	3
3	36	35	1	24	19	5	44	42	2	40	39	1	36	35	1	56	49	7	60	54	6	40	36	4
4	72	71	1	48	40	8	88	85	3	80	79	1	72	71	1	112	99	13	120	112	8	80	75	5
5	144	143	1	96	87	9	176	173	3	160	159	1	144	143	1	224	211	13	240	228	12	160	155	5
6	288	287	1	192	183	9				320	319	1	288	287	1							320	315	5

TABLE 1: (cont'd)

$q = 5.7$		$q = 3.7$		$q = 3.13$		$q = 4.1$		$q = 4.3$		$q = 3^2.5$		$q = 4.7$		$q = 7^2$	
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	12	11	1	18	18	0	12	9	3	20	20	0	21	21	0
2	24	21	3	36	35	1	24	19	5	40	38	2	42	39	3
3	48	43	5	72	71	1	48	40	8	80	77	3	84	79	5
4	96	87	9	144	143	1	96	87	9	160	155	5	168	163	5
5	192	175	17	288	287	1	192	183	9	320	311	9	336	331	5
6	384	367	17												

$q = 3.17$			$q = 5.11$			$q = 3.19$			$q = 5.9$			$q = 6.1$			$q = 3^2.7$			$q = 5.13$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	16	15	1	26	26	0	20	17	3	18	17	1	29	29	0	30	30	0	18	17	1
2	32	27	5	52	51	1	40	35	5	36	33	3	58	57	1	60	59	1	36	29	7
3	64	55	9	104	103	1	80	72	8	72	68	4	116	115	1	120	119	1	72	59	13
4	128	111	17	208	207	1	160	151	9	144	139	5	232	231	1	240	239	1	144	128	16
5	256	223	33							288	283	5							288	271	17

$q = 6.7$		$q = 3.23$		$q = 7.1$		$q = 7.3$		$q = 3.5^2$		$q = 7.11$		$q = 7.9$		$q = 3^4$	
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	33	33	0	22	21	1	35	35	0	36	36	0	20	19	1
2	66	65	1	44	41	3	70	69	1	72	67	5	40	37	3
3	132	131	1	88	83	5	140	138	2	144	136	8	80	75	5
4	264	263	1	176	168	8	280	277	3				160	151	9

$q = 8.3$		$q = 5.17$		$q = 3.29$		$q = 8.9$		$q = 7.13$		$q = 3.31$		$q = 5.19$		$q = 9.7$	
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	41	41	0	32	31	1	28	24	4	44	44	0	36	33	3
2	82	81	1	64	55	9	56	47	9	88	83	5	72	61	11
3	164	163	1	128	111	17	112	95	17	176	168	8	144	123	21
4				256	223	33	224	191	33				288	247	41

TABLE 1: (cont'd)

q = 3 ² .11			q = 101			q = 103			q = 3.5.7			q = 107			q = 109			q = 3.37			q = 113		
n	p _n	r _n d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n
0	30	29 1	50	50	0	51	51	0	24	21	3	53	53	0	54	54	0	36	34	2	56	53	3
2	60	57 3	100	99	1	102	101	1	48	39	9	106	105	1	108	105	3	72	67	5	112	105	7
3	120	116 4	200	199	1	204	202	2	96	79	17	212	211	1	216	211	5	144	136	8	224	211	13
4	240	235 5							192	165	27							288	279	9			

q = 5.23			q = 3 ² .13			q = 7.17			q = 11 ²			q = 3.41			q = 5 ³			q = 163			q = 331		
n	p _n	r _n d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n	p _n	r _n	d _n
0	44	43 1	36	33	3	48	47	1	55	55	0	40	35	5	50	50	0	81	79	2	165	165	0
2	88	85 3	72	63	9	96	91	5	110	109	1	80	67	13	100	99	1	162	159	3	330	319	11
3	176	171 5	144	128	16	192	183	9	220	219	1	160	135	25	200	199	1						

TABLE 2

RANK OF MATRIX OF SIGNATURES OF C_m^1

For each odd integer q , $3 \leq q \leq 57$, the rank of the matrix of signatures of units of the unit group C_m^1 ($m = q \cdot 2^n$, $n = 0, 2, 3, 4, \dots$) i.e. Ramachandra's units, was calculated on a VAX computer.

For each value of q the results for the matrices associated with C_m^1 , $m = q \cdot 2^n$ are arranged in the following way. For each value of n , the first column p_n gives the order of the matrix M , while the second column r_n gives the rank of M and the third column d_n gives the difference of the two, i.e. $d_n = p_n - r_n$.

TABLE 2: C'_m : RAMACHANDRA'S UNITS

$q = 3$				$q = 5$				$q = 7$				$q = 11$				$q = 13$				$q = 3.5$				$q = 17$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	1	1	0	2	2	0	3	3	0	3	3	0	5	5	0	6	6	0	4	3	1	8	8	0			
2	2	1	1	4	3	1	6	5	1	12	9	3	20	19	1	24	23	1	16	11	5	32	29	3			
3	4	3	1	8	7	1	12	9	3	24	21	3	40	39	1	48	47	1	32	23	9	64	59	5			
4	8	7	1	16	15	1	24	21	3	48	45	3	80	79	1	96	95	1	64	55	9	128	119	9			
5	16	15	1	32	31	1	48	45	3	96	93	3	160	159	1												
6	32	31	1	64	63	1	96	93	3	192	189	3															
7	64	63	1	128	127	1	192	189	3																		

$q = 19$				$q = 3.7$				$q = 23$				$q = 5^2$				$q = 3^3$				$q = 29$				$q = 31$				$q = 3.11$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	
0	9	9	0	6	5	1	11	11	0	10	10	0	9	9	0	14	11	3	15	15	0	10	10	0							
2	18	17	1	12	9	3	22	21	1	20	19	1	18	17	1	28	24	4	30	25	5	20	17	3							
3	36	35	1	24	19	5	44	41	3	40	39	1	36	35	1	56	49	7	60	53	7	40	35	5							
4	72	71	1	48	39	9	88	85	3	80	79	1	72	71	1	112	99	13	120	110	10	80	75	5							
5				96	87	9	176	173	3				144	143	1	224	211	13													
6				192	183	9																									

$q = 5.7$				$q = 37$				$q = 3.13$				$q = 41$				$q = 43$				$q = 3^2.5$				$q = 47$				$q = 3.17$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	
0	12	11	1	18	18	0	12	10	2	20	20	0	21	21	0	12	11	1	23	23	0	16	15	1							
2	24	21	3	36	35	1	24	19	5	40	38	2	42	39	3	24	21	3	46	45	1	32	27	5							
3	48	43	5	72	71	1	48	39	9	80	77	3	84	79	5	48	43	5	92	89	3	64	55	9							
4	96	87	9	144	143		96	87	9	160	155	5	168	163	5	96	87	9	184	177	7	128	111	17							

$q = 53$				$q = 5.11$				$q = 3.19$				$q = 89$			
n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n	p_n	r_n	d_n
0	26	26	0	20	18	2	18	17	1	44	44	0			
2	52	51	1	40	35	5	36	33	3	88	84	4			
3	104	103	1	80	71	9	72	67	5	176	167	9			
4				160	151	9	144	139	5						

TABLE 3

Number of χ , for which $\chi(p) = 1$ in the expression

$$[E_m^+ : C_m] = h_m^+ \prod_{\chi \neq 1} \prod_{p|m} (1 - (p)),$$

$$m = q \cdot 2^n, n = 0, 2, 3, 4, \dots$$

We observe that the $\# \chi$ for which $\chi(p) = 1$ is less than the value of d_n .

TABLE 3 : NUMBER OF X s.t. $X(p) = 1$

n^q	<u>7</u>	<u>17</u>	<u>23</u>	<u>31</u>	<u>41</u>	<u>43</u>	<u>47</u>	<u>71</u>	<u>73</u>	<u>79</u>	<u>15</u>
0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	0	2	1	2	0	0	3	0	2
3	1	2	1	3	2	2	1	1	4	1	2
4	1	4	1	5	2	2	3	1	4	3	2
5	1	4	1	9	2	2	3	1	4	3	2
6	1	4	1	9	2	2	3	1	4	3	2
7	1	4	1	9	2	2	3	1	4	3	2
8	1	4	1	9	2	2	3	1	4	3	2
9	1	4	1	9	2	2	3	1	4	3	2

(Number of $X \bmod m$ ($m = q \cdot 2^n$) for which $X(p) = 1$)